



USPTO

[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide

multiplication look up table



THE ACM DIGITAL LIBRARY


[Feedback](#) [Report a problem](#) [Satisfaction survey](#)
Terms used: [multiplication look up table](#)

Found 102,042 of 207,474

Sort results by

relevance

[Save results to a Binder](#)Try an [Advanced Search](#)Try this search in [The ACM Guide](#)

Display results

expanded form

[Search Tips](#)
☐ Open results in a new window

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

Relevance scale ☐ ☐ ☐ ☐ ☐

1 [Accelerating multi-media processing by implementing memoing in multiplication and division units](#)



Daniel Citron, Dror Feitelson, Larry Rudolph

 October 1998 **ACM SIGPLAN Notices , ACM SIGOPS Operating Systems Review ,
 Proceedings of the eighth international conference on Architectural
 support for programming languages and operating systems ASPLOS-
 VIII**, Volume 33 , 32 Issue 11 , 5
Publisher: ACM Press

Full text available: pdf (1.15 MB)

 Additional Information: [full citation](#), [abstract](#), [references](#), [citing](#), [index terms](#)

This paper proposes a technique that enables performing multi-cycle (multiplication, division, square-root …) computations in a single cycle. The technique is based on the notion of memoing: saving the input and output of previous calculations and using the output if the input is encountered again. This technique is especially suitable for Multi-Media (MM) processing. In MM applications the local entropy of the data tends to be low which results in repeated operations on the same data ...

2 [Managing routing tables for URL routers in content distribution networks](#)

Zornitza Genova Prodanoff, Kenneth J. Christensen

May 2004 **International Journal of Network Management**, Volume 14 Issue 3**Publisher:** John Wiley & Sons, Inc.Full text available: pdf (337.00 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Large-scale content distribution networks (CDNs) can be built using URL routers to redirect client HTTP requests to the nearest content source. URL routers employ very large routing tables. To improve the manageability of CDNs, we propose to use URL signatures to reduce the size of routing tables and aggressive hashing to speed-up routing look-ups.

3 [Forward rasterization](#)



Voicu Popescu, Paul Rosen

April 2006 **ACM Transactions on Graphics (TOG)**, Volume 25 Issue 2**Publisher:** ACM Press

Full text available: pdf (1.04 MB)

 Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We describe forward rasterization, a class of rendering algorithms designed for small polygonal primitives. The primitive is efficiently rasterized by interpolation between its

vertices. The interpolation factors are chosen to guarantee that each pixel covered by the primitive receives at least one sample which avoids holes. The location of the samples is recorded with subpixel accuracy using a pair of offsets which are then used to reconstruct/resample the output image. Offset reconstruction ha ...

Keywords: 3D warping, antialiasing, point-based modeling and rendering, rasterization, rendering pipeline

4 Implementation and tests of low-discrepancy sequences



Paul Bratley, Bennett L. Fox, Harald Niederreiter

July 1992 **ACM Transactions on Modeling and Computer Simulation (TOMACS)**, Volume 2 Issue 3

Publisher: ACM Press

Full text available: [pdf\(1.23 MB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Low-discrepancy sequences are used for numerical integration, in simulation, and in related applications. Techniques for producing such sequences have been proposed by, among others, Halton, Sobol', Faure, and Niederreiter. Niederreiter's sequences have the best theoretical asymptotic properties. The paper describes two ways to implement the latter sequences on a computer and discusses the results obtained in various practical tests on particular integrals.

Keywords: Niederreiter sequences, Quasi-Monte Carlo methods, low-discrepancy sequences, quasirandom sequences

5 Security: CReconfigurable finite field instruction set architecture



Nathan Jachimie, Fernando Martinez-Vallin, Jafar Saniie

February 2007 **Proceedings of the 2007 ACM/SIGDA 15th international symposium on Field programmable gate arrays FPGA '07**

Publisher: ACM Press

Full text available: [pdf\(236.94 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Reconfigurable computing can provide a significant speed-up factor to cryptographic and error correcting code algorithms. Finite field arithmetic is essential to both, but is difficult to implement efficiently. Finite field instruction set extensions and a reconfiguration framework have been constructed to enable a finite field multiplier to be regenerated via software control. A performance evaluation has been created by generating a Finite Field Extensions Unit with MicroBlaze processor in a X ...

Keywords: FSL, MicroBlaze, Xilinx, embedded development, fast simplex links, finite field arithmetic, galois fields, instruction set extensions, partial reconfiguration

6 LH*RS: a high-availability scalable distributed data structure using Reed Solomon



Codes

Witold Litwin, Thomas Schwarz

May 2000 **ACM SIGMOD Record , Proceedings of the 2000 ACM SIGMOD international conference on Management of data SIGMOD '00**, Volume 29 Issue 2

Publisher: ACM Press

Full text available: [pdf\(155.52 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

LH*RS is a new high-availability Scalable Distributed Data Structure (SDDS). The data storage scheme and the search performance of LH*RS are basically these of LH*. LH*RS manages in addition the parity information to tolerate the unavailability of $k \geq 1$

server sites. The value of k scales with the file, to prevent the reliability decline. The parity calculus uses the Reed -Solomon Codes. The storage and access performance over ...

Keywords: Reed-Solomon Codes, SDDS, high-availability, scalable

7 An adaptive cryptographic engine for internet protocol security architectures



Andreas Dandalis, Viktor K. Prasanna

July 2004 **ACM Transactions on Design Automation of Electronic Systems (TODAES)**,

Volume 9 Issue 3

Publisher: ACM Press

Full text available: pdf(264.87 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Architectures that implement the Internet Protocol Security (IPSec) standard have to meet the enormous computing demands of cryptographic algorithms. In addition, IPSec architectures have to be flexible enough to adapt to diverse security parameters. This article proposes an FPGA-based Adaptive Cryptographic Engine (ACE) for IPSec architectures. By taking advantage of FPGA technology, ACE can adapt to diverse security parameters on the fly while providing superior performance compared with softw ...

Keywords: AES, Adaptive computing, IPSec, configurable, cryptography, high performance, performance tradeoffs, reconfigurable components, reconfigurable computing, reconfigurable systems

8 Finite field manipulations in Macsyma



K. T. Rowney, R. D. Silverman

January 1989 **ACM SIGSAM Bulletin**, Volume 23 Issue 1

Publisher: ACM Press

Full text available: pdf(622.33 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We present the implementation of an extensive system of routines, in Macsyma, which allows finite field arithmetic and manipulation of symbolic objects in finite fields,

9 Case studies in embedded systems: A fast parallel reed-solomon decoder on a reconfigurable architecture



Arezou Koohi, Nader Bagherzadeh, Chengzi Pan

October 2003 **Proceedings of the 1st IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis CODES+ISSS '03**

Publisher: ACM Press

Full text available: pdf(292.18 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

This paper presents a software implementation of a very fast parallel Reed-Solomon decoder on the second generation of MorphoSys reconfigurable computation platform, which is targeting on streamed applications such as multimedia and DSP. Numerous modifications of the first-generation of the architecture have made a scalable computation and communication intensive architecture capable of extracting parallelisms of fine grain in instruction level. Many algorithms and the whole Digital Video Broadc ...

Keywords: Berlekamp algorithm, Chain search, Reed-Solomon codes, SIMD processor, reconfigurable architecture

10 High-Speed Volume Rendering Using Redundant Block Compression

Guenter Knittel

October 1995 **Proceedings of the 6th conference on Visualization '95 VIS '95**


Publisher: IEEE Computer Society

Full text available:  [pdf\(1.40 MB\)](#)  Additional Information: [full citation](#), [abstract](#), [citations](#)
[Publisher Site](#)

We present a novel volume rendering method which offers high rendering speed on standard workstations. It is based on a lossy data compression scheme which drastically reduces the memory bandwidth and computing requirements of perspective raycasting. Starting from classified and shaded data sets, we use Block Truncation Coding or Color Cell Compression to compress a block of 12 voxels into 32 bits. All blocks of the data set are processed redundantly, yielding a data structure which avoids multi ...

Keywords: Volume rendering, raycasting, data compression

11 Speeding up an overrelaxation method of division in Radix-2n machine

 Hitohisa Asai, C. K. Cheng

March 1983 **Communications of the ACM**, Volume 26 Issue 3

Publisher: ACM Press

Full text available:  [pdf\(495.52 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

For normalized floating point division, digital computers can take advantage of a division process that uses an iterative multiplying operation instead of repeated subtractions. An improvement of this division process by using accelerating constants in the overrelaxation has previously been proposed. Multiplication by a chosen accelerating constant accelerates the process of generating accurate digits of a quotient in division. We propose a further improvement by generalizing the ac ...

Keywords: Wilkes-Harvard scheme, algebraic algorithms, convergence, convergence division, iterative multiplication, overrelaxation, power series, truncation error

12 Linux and the Alpha, How to Make Your Applications Fly, Part 2

David Mosberger

November 1997 **Linux Journal**

Publisher: Specialized Systems Consultants, Inc.

Full text available:  [html\(31.16 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Linux and the Alpha, How to Make Your Applications Fly, Part 2

13 Application-specific architectures: Combining algorithm exploration with instruction set design: a case study in elliptic curve cryptography

Johann Großschädl, Paolo Ienne, Laura Pozzi, Stefan Tillich, Ajay K. Verma

March 2006 **Proceedings of the conference on Design, automation and test in Europe: Proceedings DATE '06**

Publisher: European Design and Automation Association

Full text available:  [pdf\(232.20 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#)

In recent years, processor customization has matured to become a trusted way of achieving high performance with limited cost/energy in embedded applications. In particular, Instruction Set Extensions (ISEs) have been proven very effective in many cases. A large body of work exists today on creating tools that can select efficient ISEs given an application source code: ISE automation is crucial for increasing the productivity of design teams. In this paper we show that an additional motivation fo ...

14 Dense representation of affine coordinate rings of curves with one point at infinity

S. C. Porter



July 1989 **Proceedings of the ACM-SIGSAM 1989 international symposium on Symbolic and algebraic computation ISSAC '89**

Publisher: ACM Press

Full text available: pdf(681.37 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Traditional methods of representing rational functions on curves are unwieldy and unsuitable for solution of many problems. This paper describes a simple and elegant representation of elements of the affine coordinate ring of an algebraic curve and describes efficient, easy to implement algorithms to perform addition, subtraction, multiplication and polynomial evaluation. This data structure overcomes many of the disadvantages of more unwieldy traditional representations. Elements are repre ...

15 Security: Fast authenticated key establishment protocols for self-organizing sensor networks



Qiang Huang, Johnas Cukier, Hisashi Kobayashi, Bede Liu, Jinyun Zhang

September 2003 **Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications WSNA '03**

Publisher: ACM Press

Full text available: pdf(303.05 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

In this paper, we consider efficient authenticated key establishment protocols between a sensor and a security manager in a self-organizing sensor network. We propose a hybrid authenticated key establishment scheme, which exploits the difference in capabilities between security managers and sensors, and put the cryptographic burden where the resources are less constrained. The hybrid scheme reduces the high cost public-key operations at the sensor side and replaces them with efficient symmetric- ...

Keywords: elliptic curve cryptography, key establishment, security, sensor network

16 Heresy: a virtual image-space 3D rasterization architecture



Tzi-cker Chiueh

August 1997 **Proceedings of the ACM SIGGRAPH/EUROGRAPHICS workshop on Graphics hardware HWWS '97**

Publisher: ACM Press

Full text available: pdf(1.13 MB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

Keywords: 3D scan conversion, image space, inverse projection, lazy shading, object space, speculative z-buffer sorting

17 A state-of-the-art SIMD two-dimensional FFT array processor



Mehrad Yasrebi, G. J. Lipovski

January 1984 **ACM SIGARCH Computer Architecture News , Proceedings of the 11th annual international symposium on Computer architecture ISCA '84,**

Volume 12 Issue 3

Publisher: ACM Press

Full text available: pdf(489.37 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

A novel implementation of a Two-dimensional FFT array processor is given. The reasons for its superior performance is the one-to-one and onto mapping of the problem communications topology onto the interconnection network, VLSI-based implementation, a proper choice for the number system, multiple-parallelism, and the use of packet-switching as opposed to circuit switching. A performance comparison also presented.

18 A dance of rounds

J. Phillip Benkhard

July 1991 **ACM SIGAPL APL Quote Quad , Proceedings of the international conference on APL '91 APL '91**, Volume 21 Issue 4**Publisher:** ACM PressFull text available: [pdf\(725.14 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Two different methods of getting sums of rounded numbers to add up to the rounded sum are discussed. The case of cascaded rounding, in which each number is replaced by a set of numbers to be rounded to a conforming sum, with the sum of the conforming sums itself conforming to the sum of the whole, is covered. Geometric properties of are reviewed.

19 Modeling the Power Consumption of Audio Signal Processing Computations Using Customized Numerical Representations

Roger Chamberlain, Eric Hemmeyer, Robert Morley, Jason White

March 2003 **Proceedings of the 36th annual symposium on Simulation ANSS '03****Publisher:** IEEE Computer SocietyFull text available: [pdf\(151.09 KB\)](#) Additional Information: [full citation](#), [abstract](#), [index terms](#)

This paper explores the impact that numericalrepresentation has on the power consumption of audiosignal processing applications. The motivation is digitalhearing aids, for which minimizing the powerconsumption is a critical design goal. We investigate twoaspects of this problem. First, we evaluate the validity ofusing signal transition counts to model actual powerconsumption within this problem domain, and second, wecompare the relative power consumption of multiply-accumulateoperations for seve ...

Keywords: audio signal processing, power consumption,numerical representation**20** High-precision division and square root

Alan H. Karp, Peter Markstein

December 1997 **ACM Transactions on Mathematical Software (TOMS)**, Volume 23 Issue 4**Publisher:** ACM PressFull text available: [pdf\(249.07 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

We present division and square root algorithm for calculations with more bits than are handled by the floating-point hardware. These algorithms avoid the need to multiply two high-precision numbers, speeding up the last iteration by as much as a factor of 10. We also show how to produce the floating-point number closest to the exact result with relatively few additional operations.

Keywords: division, quad precision, square root

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)Useful downloads: [Adobe Acrobat](#) [QuickTime](#) [Windows Media Player](#) [Real Player](#)